REMARKS

Claims 1-3, 7-11 and 17-21 were examined and reported in the Office Action. Claims 1-3, 7-11 and 17-21 are rejected. Claims 1, 2, 3, 7-9, 11, 17, 18, 20 and 21 are amended. Claims 1-3, 7-11 and 17-21 remain.

Applicant requests reconsideration of the application in view of the following remarks.

I. 35 U.S.C. §103(a)

It is asserted in the Office Action that claims 1-3, 7-11, and 17-21 are rejected under 35 U.S.C. §103(a) as being unpatentable over U. S. Patent No. 5,956,407 issued to Slavin ("Slavin"), in view of U. S. Patent 5,933,501 issued to Leppek ("Leppek"), further in view of U. S. Patent No. 4,797,672 issued to Kousa ("Kousa"), and further in view of Tsuji, Shigeo, *An ID-based Cryptosystem Based on the Discrete Logarithm Problem,* IEEE, 1989 ("Tsuji"). Applicant respectfully traverses the aforementioned rejection for the following reasons.

According to MPEP §2142

> [t]o establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure." (In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)).

Further, according to MPEP §2143.03, "[t]o establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. (In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974)." "*All words in a claim must be considered* in judging the patentability of that claim against the prior art." (In re Wilson, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970), emphasis added.).

That is, users each receive a different decryption process (i.e., different software executable code) for actually decrypting content actually encrypted with the main encryption process. Applicant's claimed invention turns content into cipher-content and vice versa. That is, content (e.g., data) is actually converted. Users also each have a different encryption process (i.e., different software executable code) for encrypting content to be decrypted with the main decryption process and the main key. Each of the differing decryption and encryption processes have distinct individual keys. Thus, each individual user is distributed an individual key, decryption process and encryption process customized for the specific user. Each decryption process actually decrypts an actually encrypted content differently from one another. For example, if a plurality of users wanted to download/receive the same content (e.g., a same video stream, a same audio stream, etc.), each user will have a different decryption process. Therefore, a user could not use their specific decryption process to decrypt the content that was sent/received by another user, even if the content is the same (because each is actually encrypted (i.e., each content or data received by a user is converted differently) specifically for the specific user). Each encryption process actually encrypts content differently from one another. For example, if a plurality of users wanted to upload/transmit the same content (e.g., a same video stream, a same audio stream, etc.), each user will have a different encryption process (e.g., a different application program created for the specific user). This makes it harder for someone to be able to intercept content as the content that is uploaded/transmitted by each user would need to be actually decrypted differently.

Slavin discloses a method for encrypted communication where messages are created and public keys are looked up for a recipient. The message is encoded by a first process using a first portion of the public key to generate an intermediate encoded message. Then a second encoding process uses a second portion of the public key to generate the final encoded message. The final encoded message is sent to a recipient. "To decode the message, the receiver has created a decoding key as a function of the prime factors used to create the encoding key." (Slavin, column 6, lines 31-34). That is, each recipient uses the same decoding process and different decoding keys. Slavin discloses modifying the RSA technique disclosed by Rivest et al. (4,405,829).

Slavin discloses that E_m are public encoding keys. (Slavin, column 4, lines 15-20). Slavin does not teach, disclose or suggest the limitations in claims 1, 7, 17 and 21, as listed above.

Leppek discloses a "virtual" encryption method that uses a sequence of encryptor operators to form a compound encryption operator. (Leppek, column 3, lines 48-53). Leppek does not actually encrypt or decrypt data. Leppek only wraps data with operators. (Leppek, column 4, lines 52-66). Thus, the data of Leppek is never changed, i.e., never converted to cipher. Leppek further discloses that "the data processing scheme of the present invention is effectively a `virtual` encryption and decryption scheme, as it does not actually perform any encrypting of the data, but rather assembles selected ones of a plurality of true encryption mechanisms into a cascaded sequence of successively different encryption operators." (Leppek, column 4, lines 48-59). Leppek simply uses decryption operators from a decryption operator database to decrypt the stream that was virtually encrypted with a sequence of encryptor operators. The decryption process and encryption process does not change. That is, operators change, but the same process encrypts/decrypts content. Leppek does not teach, disclose or suggest the limitations in claim 1, 7, 17 and 21, as listed above.

Moreover, it is asserted in the Office Action that the operators make up steps for the *process*. In this assertion, the term "process" is used as a method. Distinguishable, Applicant used the term process as in a software application. Applicant has, therefore, clarified the claims by using the term "application." In Leppek, the same application is used with different variables (i.e., operators) read from a database. In Leppek, the software application does not change for each individual user.

Further, even if the disclosures of Slavin and Leppek were combined, the way each cryptographic system works are so different that the combined invention would teach away from each disclosure and the combined invention could not work in reality. That is, you would create redundant security as Slavin encrypts/decrypts data and Leppek would "wrap" the encrypted data, which would further complicate and cost more to encrypt/decrypt data.

Kousa discloses using a single key (Kousa, column 4, lines 30-53). Further, it is asserted in the Office Action that it would have been obvious to "use it with one decryption process as in Kousa in the system of Slavin." Applicant's claimed invention, however, creates a plurality of decryption applications customized for each user.

Tsuji is relied on for disclosing an ID-based key distribution system. Tsuji, however, does not teach, disclose or suggest

> the decryption generating section to generate a plurality of individual decryption applications based on the main decryption section and the plurality of individual keys, each of said plurality of individual decryption applications is distributed to a corresponding user, each of said plurality of individual decryption applications is different from one another and each different individual decryption application operates to actually decrypt an encrypted content differently from one another, the main decryption section using the main key to actually decrypt content; an encryption generating section coupled to the key generating section and a main encryption section, the encryption generating section operates to generate a plurality of individual encryption applications based on the main encryption section and the plurality of individual keys, each of said plurality of individual encryption applications is distributed to a corresponding user, each of said plurality of individual encryption applications is different from one another and each different individual encryption application operates to actually encrypt a content differently from one another; the main encryption section using the main key to actually encrypt content; wherein only a one of the plurality of individual keys is used in conjunction with only a one of the plurality of decryption applications, and each of the plurality of decryption applications and its respective individual key can actually decrypt content encrypted by the main encryption section, and a one of the plurality of encryption applications can actually encrypt content to be actually decrypted by the main decryption section and the main key.

Moreover, by viewing the disclosures of Slavin, Leppek, Kousa and Tsuji, one can not jump to the conclusion of obviousness without impermissible hindsight. According to MPEP 2142,

> [t]o reach a proper determination under 35 U.S.C. 103, the examiner must step backward in time and into the shoes worn by

> the hypothetical 'person of ordinary skill in the art' when the invention was unknown and just before it was made. In view of all factual information, the examiner must then make a determination whether the claimed invention 'as a whole' would have been obvious at that time to that person. Knowledge of applicant's disclosure must be put aside in reaching this determination, yet kept in mind in order to determine the 'differences,' conduct the search and evaluate the 'subject matter as a whole' of the invention. The tendency to resort to 'hindsight' based upon applicant's disclosure is often difficult to avoid due to the very nature of the examination process. However, impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art.

Applicant submits that without first reviewing Applicant's disclosure, no thought, whatsoever, would have been made to

> the decryption generating section to generate a plurality of individual decryption applications based on the main decryption section and the plurality of individual keys, each of said plurality of individual decryption applications is distributed to a corresponding user, each of said plurality of individual decryption applications is different from one another and each different individual decryption application operates to actually decrypt an encrypted content differently from one another, the main decryption section using the main key to actually decrypt content; an encryption generating section coupled to the key generating section and a main encryption section, the encryption generating section operates to generate a plurality of individual encryption applications based on the main encryption section and the plurality of individual keys, each of said plurality of individual encryption applications is distributed to a corresponding user, each of said plurality of individual encryption applications is different from one another and each different individual encryption application operates to actually encrypt a content differently from one another; the main encryption section using the main key to actually encrypt content; wherein only a one of the plurality of individual keys is used in conjunction with only a one of the plurality of decryption applications, and each of the plurality of decryption applications and its respective individual key can actually decrypt content encrypted by the main encryption section, and a one of the plurality of encryption applications can actually encrypt content to be actually decrypted by the main decryption section and the main key.

Therefore, neither Slavin, Leppek, Kousa, Tsuji, and therefore, nor the combination of the four teach, disclose or suggest the limitations contained in Applicant's amended claims 1, 7, 17 and 21, as listed above. Since neither Slavin, Leppek, Kousa, Tsuji, and therefore, nor the combination of the four teach, disclose or suggest all the limitations of Applicant's amended claims 1, 7, 17 and 21, Applicant's amended claims 1, 7, 17 and 21 are not obvious over Slavin in view of Leppek, Kousa and Tsuji since a *prima facie* case of obviousness has not been met under MPEP §2142. Additionally, the claims that either directly or indirectly depend from amended claims 1, 7 and 17, namely claims 2-3, 8-11, and 18-20, respectively, would also not be obvious for the same reasons.

Accordingly, withdrawal of the 35 U.S.C. § 103(a) rejection for claims 1-3, 7-11, and 17-21 is respectfully requested.

CONCLUSION

In view of the foregoing, it is believed that all claims now pending, namely 1-3, 7-11 and 17-21, patentably define the subject invention over the prior art of record and are in condition for allowance and such action is earnestly solicited at the earliest possible date.

If necessary, the Commissioner is hereby authorized in this, concurrent and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2666 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17, particularly extension of time fees.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR, & ZAFMAN LLP

Dated: December 28, 2006

By: _____
Steven Laut, Reg. No. 47,736

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025
(310) 207-3800

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being submitted electronically via EFS Web on the date shown below to the United States Patent and Trademark Office.

_____
Jean Svoboda Date: December 28, 2006